

# Notice of Allowability

Application No.

10/647,640

Examiner

Benjamin E. Lanier

Applicant(s)

TAKAYAMA ET AL.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to the amendment filed 24 August 2007.
2. ☒ The allowed claim(s) is/are 1, 2, 7, 10-13, 16-26 and 31-33.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All b) ☐ Some\* c) ☐ None of the:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
    - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
    - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

## Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date \_\_\_\_\_
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

### **DETAILED ACTION**

#### ***Response to Amendment***

1. Applicant's amendment filed 24 August 2007 amends claims 1, 2, 7, 10-13, 16, 17, 19-26, 31-33. Claims 3-6, 8, 9, 14, 15, and 27-30 have been cancelled.

#### ***Response to Arguments***

2. Applicant's argument that the claim amendments have overcome the §112, second paragraph, rejections of claims 7, 11-13, 19, 22-24 has been fully considered and is persuasive. The overcome the §112, second paragraph, rejections of claims 7, 11-13, 19, 22-24 have been withdrawn.

### **EXAMINER'S AMENDMENT**

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.
4. Authorization for this examiner's amendment was given in a telephone interview with Ronald E. Brown on 11 September 2007.

The application has been amended as follows:

Change "authentication information" to "said authentication information" on line 8 of claim 1.

Change "user" to "said user" on line 8 of claim 1.

Change "master key" to "said master key" on line 11 of claim 2.

Delete "further encoding by an irreversible calculation process" on line 5 of claim 7.

Delete "(F) wherein" on line 6 of claim 7.

Delete "said" from line 7 of claim 7.

Add "on said concatenation" after "process (G)" on line 8 of claim 7.

Change "authentication information" to "said authentication information" on line 9 of claim 7.

Change "encrypted part" to "an encrypted part" on line 3 of claim 10.

Add "key" after "decryption" on line 3 of claim 16.

Change "received electronic" to "said received electronic" on line 7 of claim 16.

Change "wherein authentication" to "wherein said authentication" on line 4 of claim 20.

Change "said first irreversible" to "a first irreversible" on line 5 of claim 20.

Change "a" to "an" on line 6 of claim 20.

Change "said signature" to "signature" on line 6 of claim 23.

Add "said value" before "authentication" on line 3 of claim 24.

Change "value" to "said value" on line 17 of claim 25.

Change "said decryption key of" to "a decryption key from" on line 2 of claim 26.

Change "a" to "said" on line 7 of claim 26.

Add "said" before "authentication" on line 9 of claim 26.

Add "said" before "authentication" on line 10 of claim 26.

Change "a decryption key" to "said decryption key" on line 10 of claim 26.

Add "said" before "master" on line 11 of claim 26.

Add "said" before "received" on line 11 of claim 26.

Add "value" before "authentication" on line 3 of claim 31.

Art Unit: 2132

Change “said” to “an” on line 5 of claim 31.

Add “an” before “encrypted” on line 14 of claim 31.

Delete “said” before “authentication” on line 16 of claim 31.

Add “said” before “value” on line 16 of claim 31.

Add “said” before “received” on line 16 of claim 31.

Add “said” before “generated” on line 17 of claim 31.

Add “said” before “user” on line 4 of claim 32.

Add “said” before “received” on line 9 of claim 32.

Add “said” before “generated” on line 10 of claim 32.

Change “authentication process” to “said authentication process” on line 6 of claim 33.

***Allowable Subject Matter***

5. Claims 1, 2, 7, 10-13, 16-26, 31-33 are allowed.

The following is an examiner’s statement of reasons for allowance: The claimed invention generally concerns user authentication wherein the authentication side transmits a random number to the user. The user hashes an authentication value with a first one-way hash function and encrypts the hash. The user then concatenates the encrypted hash with the received random number and hashes the concatenation with a second one-way hash function to be transmitted to the authentication side along with the encrypted hash. The authentication side then decrypts the received hash, concatenates the decrypted hash with the random number that was previously transmitted to the user in question, hashes the concatenation with the second one-way hash function, and compares the hashed concatenation with the hashed concatenation received

Art Unit: 2132

form the user. If the authentication side verifies that the hashes are identical, the user is authenticated.

6. The closes prior art (Larsen, U.S. Publication No. 2004/0098627) discloses a similar user authentication system wherein the authentication side transmits a random number to the user (Figure 13, 340). The user concatenates the received random number with a password (Figure 13, 344), hashes the concatenation (Figure 13, 344), and transmits the hash to the authentication side (Figure 13, 346). The authentication side then retrieves the previously transmitted random number (Figure 13, 350), the password associated with the user (Figure 13, 352), concatenates the random number and the password (Figure 13, 354), hashes the concatenation (Figure 13, 354), and compares the hash value with the hash received from the user (Figure 13, 356). If the hashes match, then the user is authenticated (Figure 13, 360).

7. The prior art does not disclose or make obvious hashing the password with a first one-way hash function prior to being concatenated with the received random number and hashed with a second one-way hash function. The prior art also does not disclose or make obvious that this concatenated hash is transmitted to the authentication side along with the encrypted first hash such that the authentication side decrypts the encrypted hash, concatenates the decrypted hash with the previously transmitted random number, hashes the concatenation with the second one-way hash function, and compares the hashed concatenation with the hashed concatenation received from the user in order to authentication the user.

8. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue

Art Unit: 2132

fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

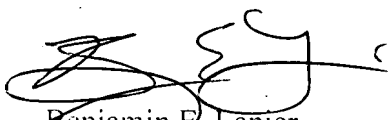
*Conclusion*

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805.

The examiner can normally be reached on M-Th 6:00am-4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Benjamin E. Lanier